Strong Privacy for RFID Systems from Plaintext-Aware Encryption

Serge Vaudenay

EPFL
CH-1015 Lausanne, Switzerland
http://lasec.epfl.ch

Abstract. Modeling privacy for RFID protocols went through different milestones. One pretty complete model was proposed by Vaudenay at ASIACRYPT 2007. It provides a hierarchy of privacy levels, depending on whether corruption is addressed by the protocol and on whether the return channel from the reader is available. The strongest notion of privacy was proven to be impossible to achieve, but the counterexample which was given was not convincing. Somehow, it showed that the requirements for strong privacy were unnecessarily too high. Several amendments were considered until a slight change in the definition which was proposed at CANS 2012. There, the simulator (blinder) was given access to the adversary's random tape, making him able to read his mind. Thanks to plaintext-aware encryption, we can now prove that strong privacy is possible.

1 RFID Protocols and Privacy Issues

RFID protocols must face to contradictory requirements. On the one hand, RFID tags should be able to securely authenticate to a reader (or a network of readers). On the other hand, nobody else should be able to identify or trace tags as they move and interact with the environment. Since communication is wireless, modeling these requirements, then providing provably secure protocols, are challenging tasks for cryptographers.

We assume that tags are simple devices which can only respond to requests and do simple operations and data storage. They interact with readers. Readers are connected to a central server which maintains a database. Typically, we focus on the tag-reader protocol and assume that the reader network system is perfectly secure.

Ideally, an RFID protocol would be a two-path protocol in which the reader sends a challenge, then the tag answers. The tag may remain stateless. Otherwise, writing in memory would induce an overhead.

Clearly, if the response function is deterministic, one can easily trace a tag by replaying a challenge: the answer to the same challenge by the same tag will always be the same. So, the response function must be randomized.

Now, if the adversary can corrupt all tags and read their memory at the end of the attack, it may be the case that what leaks enables to identify which tag answered, when we use symmetric cryptography. To avoid that, [5] considered stateful protocols in which the key which was used to respond is updated in a one-way manner. This is the notion of *forward privacy*.

In [1], the authors consider that corruption may occur at earlier stages. I.e., not only at the end of the attack.

Finally, [3] notices that an adversary could try do desynchronize a stateful tag from its database so that it will no longer be identified. Then, if the adversary gets whether readers identify tags through a *return channel* (e.g., by looking at whether a door opens or not, if the reader is used for access control to buildings), then the protocol by [5] offers no longer privacy.

2 The 2007 Privacy Model(s)

We review here the formalism from [7].

Adversaries are assumed to have full control on the communication with tags and readers. They can activate the reader to start a protocol. They can draw anonymous tags with a chosen distribution. They can communicate with drawn tags. They can initiate the creation of tags which belong to the system or not. They can free drawn tags so that they may be drawn again. They may corrupt drawn tags to retrieve their memory. They may read the return channel from the reader to see whether the protocol succeeded.

We distinguish 2×3 classes of adversaries. On one dimension, we distinguish whether they use the return channel or not. Adversaries not using it are called *narrow* adversaries. Others are *wide* adversaries. On the other dimension, we distinguish the type of corruption. Adversaries using no corruption are called *weak*. Adversaries making all corruptions at the end of their attack are called *forward*. Others are called *strong*.

The (strongest) security notion implies that for any wide-strong adversary, the probability that there is a reader protocol which succeeds to identify a tag but that tag has no matching conversation is negligible.

In the privacy game, we consider an adversary running the attack, then getting the table of ID's of all drawn tags, then producing a bit. Privacy implies that the bit they produce would be the same if all communication and return channels were simulated. Concretely, privacy holds if for all adversaries, there exists a simulator (called a *blinder*) who sees the interaction between the adversary and the system but simulates all messages from tags, the reader, and the return channel; which blinder would be such that the blinded experiment produces indistinguishable outcomes form the un-blinded one.

We can achieve security and wide-weak privacy with a simple protocol based on a PRF. Protocols like [5] may achieve security and narrow-forward privacy in the random oracle model. Finally, we can achieve security, narrow-strong privacy, and wide-forward privacy at the same time using a public-key cryptosystem which is IND-CCA secure.

This protocol, called the PKC protocol, works as follows. A public/secret key pair is generated. The reader receives the secret key K_S while the public one K_P is stored in all tags. Each tag receives an ID and a secret K which is also stored in the database. To authenticate, the tag receives a random challenge a and encrypts, with K_P, the ID, K, and a together. The ciphertext is the response. The reader can decrypt it with K_S, check that the challenge is correct, then check the entry in the database.

Tag		**System**
state: K_P, ID, K		**secret key:** K_S
		$\{\ldots,(\mathsf{ID},K),\ldots\}$
	$\xleftarrow{a}$	pick a
$c = \mathsf{Enc}_{K_P}(\mathsf{ID}\|K\|a)$	$\xrightarrow{c}$	$\mathsf{Dec}_{K_S}(c) = \mathsf{ID}\|K\|a$
		check a, (ID,K)
		output: ID

It was shown that security and wide-strong privacy were impossible to achieve at the same time. To prove that, we first consider a wide-strong adversary who creates a legitimate tag, then corrupt it. Then, he simulates the creation of an illegitimate tag. He flips a coin and, based on the outcome, decides to simulate one tag or the other to the reader. Then, the result channel gives a bit and the adversary compares it with the coin flip to produce the result.

If the protocol was wide-strong private, there would be a blinder to simulate the reader and yield whether or not the simulated tag was the legitimate one or not. This blinder would work based on

the state of the legitimate tag (obtained from corruption). Then, this blinder could be used by a new adversary.

The new adversary creates two legitimate tags, corrupt them both, then draw one or the other at random, and interact with the drawn tag. Simulating the previous blinder would make it possible to identify the tag. Then, the adversary would check from the table of ID's if this was correct. Clearly, this new adversary cannot be blinded.

One crucial point in this proof is that the first adversary is querying the result channel for a bit that he already knows but that a blinder has troubles to simulate. This was observed by [4] who suggested that adversary should not ask questions to the environment for which they know the answer. This is the notion of *wise* adversary. However, it is pretty complicated to formalize it.

3 The 2012 Amendment

An alternate amendment was proposed in [6]. There, the definition of the blinder was updated so that the blinder would have access to the adversary's random tape. Thus, the blinder could compute the same information that the adversary knows, and he would therefore be able to simulate the answers from the environment that the adversary knows. Somehow, the blinder would read the adversary's mind.

With this new formalism, we can prove that the above PKC protocol provides wide-strong privacy (in the updated formalism), when the cryptosystem is IND-CPA secure and PA2-secure. PA2-security stands for plaintext awareness. The idea is that by reading the adversary's random tape and the ciphertexts that they produce, a blinder could deduce which plaintext was encrypted by the adversary.

We could further show that some IND-CCA-secure cryptosystems which are not PA2-secure do not make the PKC protocol wide-strong private.

4 Conclusion

In [2], another privacy model was presented. This model is much simpler as it is not based on simulation. However, it was shown that IND-CCA-secure cryptosystems make the PKC protocol wide-strong private in this model. This suggests that there is a gap between the two models. So far, no separating protocol has shown to leak any private information in a real-life setting. Providing such a protocol is an open problem.

References

1. G. Avoine, E. Dysli, P. Oechslin. Reducing Time Complexity in RFID Systems. In *Selected Areas in Cryptography'05*, Kingston, Ontario, Canada, Lecture Notes in Computer Science 3897, pp. 291–306, Springer-Verlag, 2006.
2. J Hermans, A. Pashalidis, F. Vercauteren, B. Preneel. A New RFID Privacy Model. In *Computer Security - ESORICS 2011*, Leuven, Belgium, Lecture Notes in Computer Science 6879, pp. 568–587, Springer-Verlag, 2011.
3. A. Juels, S. Weis. Defining Strong Privacy for RFID. Technical report 2006/137, IACR, 2006. http://eprint.iacr.org/2006/137
4. C.Y. Ng, W. Susilo, Y. Mu, R. Safavi-Naini. RFID Privacy Models Revisited. In *Computer Security - ESORICS 2008*, Málaga, Spain, Lecture Notes in Computer Science 5283, pp. 251–266, Springer-Verlag, 2008.
5. M. Ohkubo, K. Suzuki, S. Kinoshita. Cryptographic Approach to a Privacy Friendly Tag. Presented at the *RFID Privacy Workshop*, MIT, USA, 2003.
6. K. Ouafi, S. Vaudenay. Strong Privacy for RFID Systems from Plaintext-Aware Encryption. To appear in the proceedings of CANS'12.
7. S. Vaudenay. On Privacy Models for RFID. In *Advances in Cryptology ASIACRYPT'07*, Kuching, Malaysia, Lecture Notes in Computer Science 4833, pp. 68–87, Springer-Verlag, 2007.